PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-277855
(43)Date of publication of application : 02.10.1992

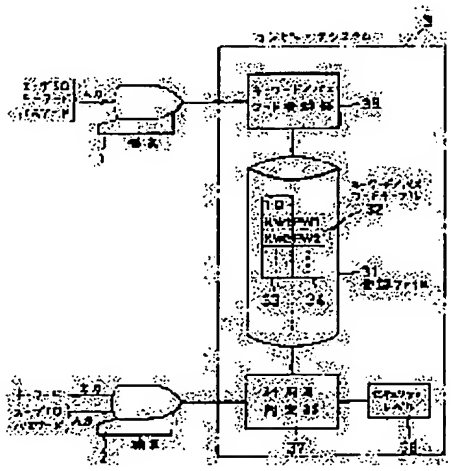
(51)Int.Cl. G06F 15/00

(21)Application number : 03-038641
(22)Date of filing : 05.03.1991

(71)Applicant : TOSHIBA CORP
(72)Inventor : FURUKAWA AKIRA

(54) LOG-IN CONTROL SYSTEM

(57)Abstract:
PURPOSE: To enable log-in only for a specified user decided by the security level among the plural users to use the same user ID and further to extremely improve an effect for preventing the illegal log-in to a system.
CONSTITUTION: When a log-in request with the input of the user ID is applied from a terminal 2 to a computer system 3, corresponding to the user ID, passwords to be paired with respective keywords contained in a certain number of paired keywords/passwords corresponding to the security level shown by a security level set part 32 are successively inputted among the plural pairs of keywords/passwords registered on a keyword/password table 32 of a registration file 31, and a user judgement part 37 judges it by comparing and collating the passwords whether the user is legal or not.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－277855

(43)公開日　平成４年(1992)10月２日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｂ	7323－5Ｌ		

審査請求　未請求　請求項の数２(全　５　頁)

(21)出願番号　特願平3－38641

(22)出願日　平成３年(1991)３月５日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　古川　彰
東京都府中市東芝町１番地　株式会社東芝府中工場内

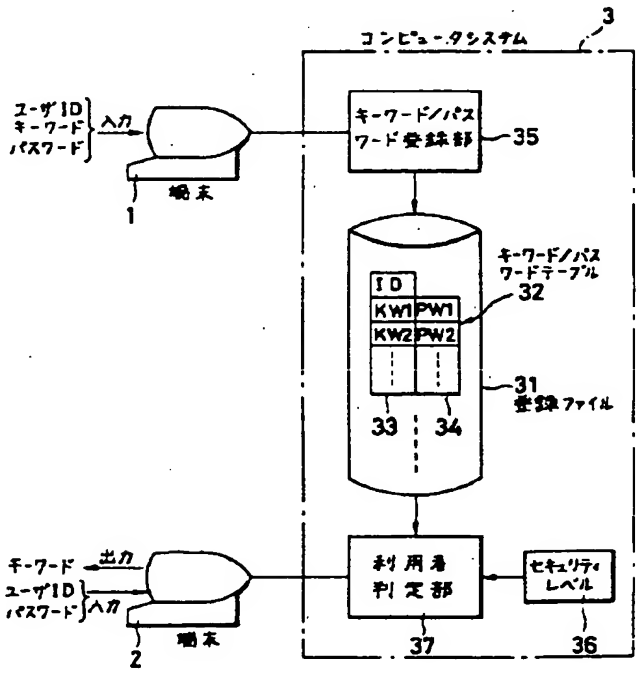
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　ログイン制御方式

(57)【要約】

【目的】同一ユーザＩＤを利用する複数の利用者のうち、セキュリティレベルで決まる特定の利用者だけがログインでき、しかもシステムへの不正ログインの防止効果を著しく高められるようにすることである。

【構成】ユーザＩＤの入力を伴うログイン要求が端末２からコンピュータシステム３に対して行われると、そのユーザＩＤに対応して登録ファイル３１のテーブル３２に登録されている複数組のキーワード／パスワード対のうちのセキュリティレベル設定部３２の示すセキュリティレベルに応じた数のキーワード／パスワード対にそれぞれ含まれている各キーワードと対になるパスワードを順次入力させ、パスワードの比較照合により正当な利用者であるか否かを利用者判定部３７にて判定する構成としたものである。



1

【特許請求の範囲】

【請求項１】　コンピュータシステムへのログインをユーザＩＤとパスワードによって制御するログイン制御方式において、上記コンピュータシステムのセキュリティレベルを設定するためのセキュリティレベル設定手段と、各ユーザＩＤ毎に複数組のキーワードとパスワードとの対を登録するためのキーワード／パスワード対登録手段と、利用者からのログイン要求時に、その利用者のユーザＩＤに対応して登録されている複数組のキーワード／パスワード対のうちの上記セキュリティレベルに応じた数のキーワード／パスワード対にそれぞれ含まれている各キーワードと対になるパスワードを順次入力させて正当な利用者であるか否かを判定し、ログインを制御する利用者判定手段と、を具備することを特徴とするログイン制御方式。

【請求項２】　上記利用者判定手段は、ユーザＩＤに対応して登録されている複数組のキーワード／パスワード対の中からセキュリティレベルに応じた数の任意のキーワード／パスワード対を任意の順序で選択し、そのキーワード／パスワード対に含まれているキーワードと対になるパスワードを選択順に入力させることを特徴とする請求項１記載のログイン制御方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、コンピュータシステムへのログインをユーザＩＤとパスワードによって制御するのに好適なログイン制御方式に関する。

【０００２】

【従来の技術】従来、コンピュータシステムでは、不特定多数の者が不正にログインできないように、ユーザＩＤと単一のパスワードを用いた方式により利用者のログインを制御するのが一般的であった。即ち従来は、利用者がユーザＩＤを入力してログインを要求すると、システム側では利用者に対し、そのユーザＩＤに対応する唯一のパスワードの入力を促す。そこで利用者がパスワードを入力すると、システム側は、入力されたパスワードとユーザＩＤに対応して予め登録されているパスワードとを比較照合し、両パスワードが一致している場合に限り、ログインを許可する。

【０００３】このようなログイン制御では、ユーザＩＤとパスワードを知っている利用者の誰もが自由にシステムにログインできてしまう。しかも、パスワードとして意味のある単語を設定することが多いため、電子辞書等により比較的容易にパスワードの解析を行うことができ、正当な利用者でなくてもログインが可能となるという問題があった。

【０００４】

【発明が解決しようとする課題】上記したように、ユーザＩＤと単一のパスワードを用いて利用者のログインを制御する従来の方式では、ユーザＩＤと単一のパスワードを知ってさえいれば誰でも自由にログインでき、しかもパスワードとして通常意味のある単語が用いられることからパスワードの解析が比較的容易に行えるので、正当な利用者でなくてもコンピュータシステムに不正にログインできるおそれが多分にあった。また、コンピュータシステムのセキュリティレベルに応じて、利用者を限定することもできなかった。

【０００５】この発明は上記事情に鑑みてなされたものでその目的は、同一ユーザＩＤを利用する複数の利用者のうち、セキュリティレベルで決まる特定の利用者だけがログインできるようなログイン制御方式を提供することにある。この発明の他の目的は、コンピュータシステムへの不正ログインの防止効果を著しく高めることができるログイン制御方式を提供することにある。

【０００６】

【課題を解決するための手段】この発明は、各ユーザＩＤ毎に複数組のキーワードとパスワードとの対を予め登録しておき、利用者からのログイン要求時には、その利用者のユーザＩＤに対応して登録されている複数組のキーワード／パスワード対のうちのコンピュータシステムのセキュリティレベルに応じた数の（例えば任意の）キーワード／パスワード対にそれぞれ含まれている各キーワードと対になるパスワードを（例えば任意の順序で）順次入力させて正当な利用者であるか否かを判定し、ログインを制御するようにしたことを特徴とするものである。

【０００７】

【作用】上記の構成において、利用者からログインが要求されると、その利用者のユーザＩＤに対応して登録されている複数組のキーワード／パスワード対のうちの、システムのセキュリティレベルで決まる数（レベルが高いほど大きな値となる）の（例えば任意の）キーワード／パスワード対が（例えば任意の順序で）選択され、この選択された各キーワード／パスワード対にそれぞれ含まれているキーワードを（例えば選択順に）順次画面表示することにより、そのキーワードと対になるパスワードの入力を利用者に対して促す。そして利用者が、画面表示されているキーワードと対になる正しいパスワードを、キーワードが切り替わる毎に次々と入力することにより、ログインが許可される。

【０００８】このように、上記の構成においてコンピュータシステムにログインするためには、利用者は、システム側から順次提示される複数のキーワードにそれぞれ対応する正しいパスワードを、そのキーワードと対にして全て知っていなければならない。しかも、知っているべきパスワードの数は、セキュリティレベルが高くなるほど多くなる。

【０００９】このため、同一ユーザＩＤを利用する複数の利用者のうち、特定の利用者だけに多くのキーワード／パスワード対を知らせておくことにより、セキュリテ

ィレベルに応じた特定利用者だけのシステム利用に限定することを可能とする。

【００１０】また、ユーザＩＤに対応して登録されていたキーワードを、システムにより任意の順序で与えるようにするならば、単に複数のパスワードだけを知ることができたとしても、各キーワードとの対で知っていない限り、容易にはログインできず、不正ログインが防止できる。

【００１１】

【実施例】図１はこの発明を適用するシステムの一実施例を示す機能ブロック構成図である。同図において、１，２は端末、３は端末１，２によって利用されるコンピュータシステム（ホスト装置）である。端末１は、ユーザＩＤ毎にキーワードとパスワードとの対（キーワード／パスワード対）を登録するための登録操作に用いられる。また端末２は、ログイン要求のためのユーザＩＤ入力、ログイン要求時にコンピュータシステム３（内の後述する利用者判定部３７）から出力されキーワードの表示、および表示されたキーワードに対応するパスワードの入力等に用いられる。なお、端末１，２は説明の便宜上独立して設けられているが、１つの端末で代用できることは勿論である。

【００１２】コンピュータシステム３は、ユーザＩＤ毎に複数のキーワード／パスワード対が登録される登録ファイル３１を有している。この登録ファイル３１には、ユーザＩＤ毎にキーワード／パスワードテーブル３２が生成される。このテーブル３２の各エントリは、キーワード（ＫＷｉ）の登録フィールド（キーワード登録フィールド）３３とパスワード（ＰＷｉ）の登録フィールド（パスワード登録フィールド）３４を持つ。

【００１３】コンピュータシステム３はまた、端末１から入力されたキーワード／パスワード対をユーザＩＤに対応させてキーワード／パスワードテーブル３２に登録するキーワード／パスワード登録部３５、およびコンピュータシステム３のセキュリティレベルが同システム３によって設定されるセキュリティレベル設定部３６を有している。このセキュリティレベルは、例えば使用時間帯に応じて適宜変更されるものである。また、コンピュータシステム３を利用したシステム開発等の業務の重要さの程度に応じて、セキュリティレベルを変更することも可能である。

【００１４】コンピュータシステム３は更に、端末２を用いて行われる利用者からのログイン要求時に、その利用者の正当性を判定してログインの許可を決定する利用者判定部３７を有する。この利用者判定部３７は、端末２から入力されたユーザＩＤに対応するキーワード／パスワードテーブル３２の登録内容のうち、セキュリティレベル設定部３６の示すセキュリティレベルに応じた数の任意のキーワード／パスワード対にそれぞれ含まれている各キーワードと対になるパスワードを任意の順序で端末２から入力させて正当な利用者であるか否かを判定するものである。

【００１５】図２はキーワード／パスワードテーブル３２の内容例を示す図、図３はログイン要求時における端末２の入出力内容例を示す図、図４はログイン要求時における利用者判定部３７の処理手順を示すフローチャートである。

【００１６】次に、図１の構成の動作を、（１）キーワード／パスワード対登録要求時と、（２）ログイン要求時のそれぞれについて、図２乃至図４を適宜参照して説明する。

【００１７】（１）キーワード／パスワード対登録要求時の動作

キーワード／パスワード対の登録が可能な特定利用者（管理者）は、端末１を用いて特別の手続き（この手続きの内容については本発明に関係しないため説明を省略）を行うことにより、コンピュータシステム３をキーワード／パスワード対登録モードに設定する。ここでは、利用者は端末１を操作してユーザＩＤを指定し、そのユーザＩＤについてのキーワードとパスワードとの対を複数組、順に入力する。

【００１８】コンピュータシステム３内のキーワード／パスワード対登録部３５は、端末１から入力されたキーワードとパスワードの対を、指定されたユーザＩＤに対応して登録ファイル３１上に作成したキーワード／パスワード対テーブル３２のキーワード登録フィールド３３，パスワード登録フィールド３４に登録していく。

【００１９】これにより、ユーザＩＤとして例えば“ｏｃｅａｎ”が指定され、このユーザＩＤについてのキーワード／パスワードの対として、例えば“ｐｒｏｊｅｃｔ”／“ｌａｎｇｕａｇｅ”，……，“ｓｅａｓｏｎ”／“ｓｕｍｍｅｒ”……が順に入力された場合であれば、登録ファイル３１には図２に示すような内容のキーワード／パスワードテーブル３２が作成される。

【００２０】（２）ログイン要求時の動作

さて、利用者（キーワード／パスワード対の登録時の利用者と同一とは限らない）は、コンピュータシステム３を利用したい場合には、同システム３に対して端末２によりユーザＩＤの入力を伴うログイン要求を行う。ここでは、ユーザＩＤとして図３に示すように“ｏｃｅａｎ”が入力されたものとする。

【００２１】端末２によりログインが要求されると、コンピュータシステム３内の利用者判定部３７が起動される。これにより利用者判定部３７は、照合回数を管理するための例えばソフトウェアカウンタである照合回数カウンタｎ（図示せず）の値を“０”クリアする（ステップＳ１）。次に利用者判定部３７は、ログイン要求を行った利用者の（操作により端末２から入力された）ユーザＩＤ“ｏｃｅａｎ”に対応して登録ファイル３１内に作成されている図２に示すキーワード／パスワードテーブ

5

ル32（のキーワード登録フィールド33）から、登録キーワードの1つをランダムに検索し、それを端末2に表示することで、そのキーワードと対になるパスワードの入力を促す（ステップS2）。ここでは、図3に示すようにキーワード“season”が検索されて、端末2に表示されたものとする。

【0022】利用者は、端末2にキーワードが表示されると、そのキーワードと対になるパスワードを端末2より入力する。ここでは、キーワードとして“seaso n”が表示されていることから、正当な利用者であれば、“season”と対になる“summer”をパスワードとして入力する（図3参照）。

【0023】利用者判定部37は、キーワード表示に応じて端末2から入力されるパスワードを入力し（ステップS3）、この入力パスワードと、表示したキーワードと対になってキーワード／パスワードテーブル32のパスワード登録フィールド34に登録されているパスワードとを、比較照合する（ステップS4）。もし、両パスワードが一致していなければ、利用者判定部37は不正な利用者によるログイン要求であるものとして、ログインの許可を与えない。

【0024】一方、ステップS4の比較照合の結果、両パスワードが一致していることを判定した場合には、利用者判定部37は照合回数カウンタnの値を＋1し（ステップS5）、この＋1後のnの値（ここでは「1」）がセキュリティレベル設定部36に設定されているセキュリティレベルに一致するか否かを判定する（ステップS6）。今、コンピュータシステム3のセキュリティレベルが「2」であるものとすると、ステップS6の判定はNOとなる。この場合、利用者判定部37はテップS2に戻り、キーワード／パスワードーブル32（のキーワード登録フィールド33）から、登録キーワードの1つをランダムに検索し（但し、先に検索したキーワードは除く）、それを端末2に表示する。ここでは、2つ目のキーワードとして図3に示すように“project”が検索されて、端末2に表示されたものとする。

【0025】利用者は、端末2に2回目のキーワード表示が行われると、1回目のキーワード表示の場合と同様に、そのキーワードと対になるパスワードを端末2より入力する。キーワードとして“project”が表示されているこの例では、正当な利用者であれば、“project”と対になる“language”をパスワードとして入力する（図3参照）。

【0026】利用者判定部37は、端末2から入力されるパスワードを入力し（ステップS3）、この入力パスワードと、表示したキーワードと対になってキーワード／パスワードテーブル32に登録されているパスワードとを、比較照合する（ステップS4）。もし、両パスワードが一致していれば、利用者判定部37は照合回数カウンタnの値を＋1し（ステップS5）、この＋1後の

6

nの値（ここでは「2」）がセキュリティレベル設定部36の示すセキュリティレベル（ここでは「2」）に一致するか否かを判定する（ステップS6）。この例のように一致している場合、利用者判定部37は、セキュリティレベルで示される数のパスワードが、ランダムに検索された登録キーワードに正しく対応して順に入力され、したがってセキュリティレベルに応じた正当な利用者によるログイン要求であったものとして、コンピュータシステム3へのログインを許可する。

【0027】なお、前記実施例では、入力すべきパスワードの回数が、セキュリティレベル設定部36に設定されるセキュリティレベルにより直接示される場合について説明したが、これに限るものではなく、セキュリティレベルが高いほど、入力すべきパスワードの回数が多くなるように設定されていればよい。

【0028】

【発明の効果】以上詳述したようにこの発明によれば、利用者からのログイン要求時に、その利用者のユーザIDに対応して登録されている複数組のキーワード／パスワード対のうちのシステムのセキュリティレベルに応じた数のキーワード／パスワード対にそれぞれ含まれている各キーワードと対になるパスワードを順次入力させて正当な利用者であるか否かを判定するようにしたので、利用者はセキュリティレベルが高い場合ほど、種々のキーワードに対応させて多くのパスワードを入力しなければならず、したがって多数のパスワードを知っている特定の利用者のみにセキュリティレベルに応じてログイン許可を与えることができる。

【0029】また、この発明によれば、セキュリティレベルが高くなるほど、キーワードとパスワードとの対を多数知っていなければならないため、コンピュータシステムへの不正ログインの防止効果を著しく高めることができる。この効果は、パスワードの入力順を決定する登録キーワードの検索順序をランダムにするならば、一層高められる。

【図面の簡単な説明】

【図1】この発明を適用するシステムの一実施例を示す機能ブロック構成図。

【図2】図1のキーワード／パスワードテーブル32の内容例を示す図。

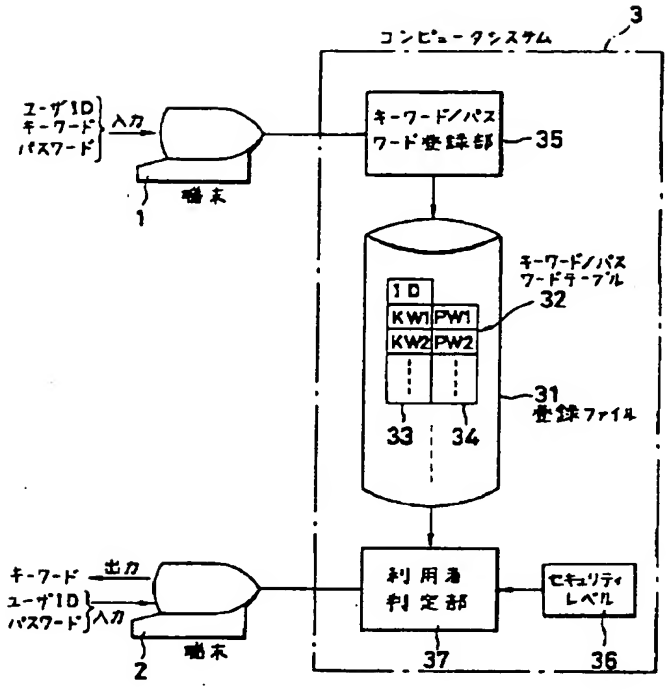
【図3】ログイン要求時における図1の端末2の入出力内容例を示す図。

【図4】ログイン要求時における利用者判定部37の処理手順を示すフローチャート。

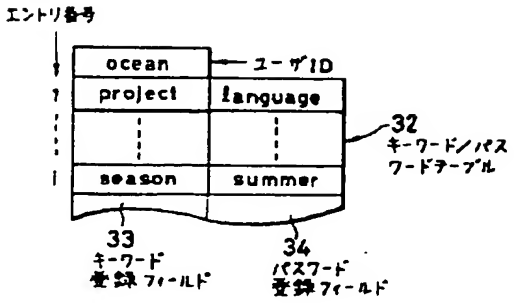
【符号の説明】

1，2…端末、3…コンピュータシステム、31…登録ファイル、32…キーワード／パスワードテーブル、35…キーワード／パスワード登録部、36…セキュリティレベル設定部、37…利用者判定部。

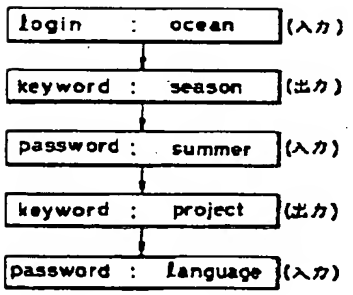
【図1】


3
コンピュータシステム
ユーザID
キーワード
パスワード
入力
端末
1
キーワード/パスワード登録部
35
キーワード/パスワードテーブル
ID
KW1
PW1
KW2
PW2
32
31
登録ファイル
33
34
キーワード
出力
ユーザID
パスワード
入力
端末
2
利用者判定部
セキュリティレベル
37
36

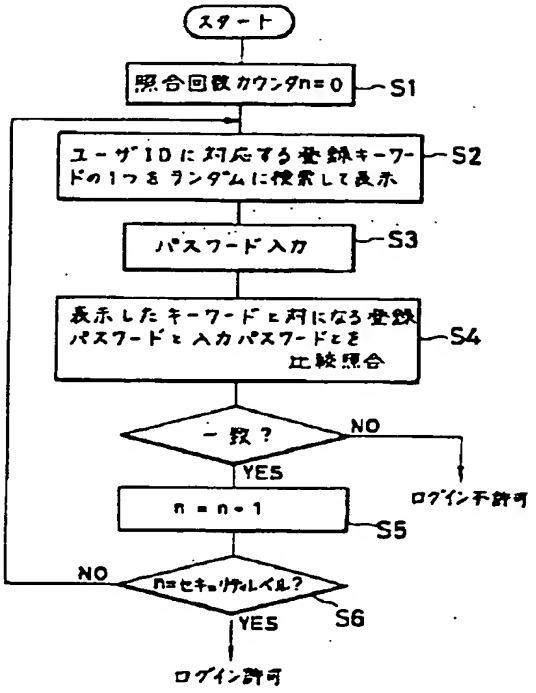
【図2】


エントリ番号
ocean
ユーザID
project
language
season
summer
32
キーワード/パスワードテーブル
33
キーワード登録フィールド
34
パスワード登録フィールド

【図3】


login : ocean (入力)
keyword : season (出力)
password : summer (入力)
keyword : project (出力)
password : language (入力)

【図4】


スタート
照合回数カウンタn=0
S1
ユーザIDに対応する登録キーワードの1つをランダムに検索して表示
S2
パスワード入力
S3
表示したキーワードと対になる登録パスワードと入力パスワードとを比較照合
S4
一致？
NO
YES
ログイン不許可
n=n-1
S5
NO
n=セキュリティレベル?
S6
YES
ログイン許可

Our Ref.: OP1710-US

(Prior Art Reference)

Japanese Patent laid-Open Publication No.04-277855

Laid-open Date: October 2, 1992

Title of the Invention: LOG-IN CONTROL SYSTEM

Application Number: 03-038641

Date of Filing: March 5, 1991

Applicant: ID No. 000003078

TOSHIBA CORP

Kawasaki-shi, Kanagawa, Japan

Inventor: Akira FURUKAWA

Pertinent Description ([0016]-[0027])

[0016]

Next, the operations according to the configuration in Fig. 1 are explained with respect to (1) when a keyword/password-pair registration request is made, and (2) when a login request is made. Fig. 2 through Fig. 4 are referenced where appropriate.

[0017]

Operations at the time of (1) when the keyword/password-pair registration request is made:

A specific user who is able to register a keyword/password pair (i.e., a administrator) uses a terminal 1 to perform specific procedures (the content of these procedures is irrelevant to the present invention and thus explanation thereof is omitted), so as

to put a computer system 3 into a keyword/password-pair registration mode. Here, the user operates the terminal 1 to designate a user ID, and then sequentially inputs multiple keyword and password pairs for that user ID.

[0018]

A keyword/password pair registration unit 35 inside the computer system 3 registers, in correspondence with the designated ID, the keyword/password pair that was inputted from the terminal 1, into a keyword registration field 33 and a password registration field 34 in a keyword/password pair table 32 which has been prepared in a registration file 31.

[0019]

Accordingly, in a case where "ocean" for example is designated as the user ID and "project"/"language", ..., "season"/"summer" ... for example are sequentially inputted as the keyword/password pair for this user ID, the keyword/password table 32 such as shown in Fig. 2 will be prepared in the registration file 31.

[0020]

(2) Operations at the time of the login request:

When a user (who is not necessarily the same as the user at the time when the registration of the keyword/password pair was performed) wants to use the computer system 3, a terminal 2 is used to perform a login request to the computer system 3 along with inputting the user ID. Here, it is assumed that "ocean" has been

inputted as the user ID, as shown in Fig. 3.

[0021]

When the login has been requested using the terminal 2, a user determination unit 37 in the computer system 3 is loaded. When this occurs, a value represented by a comparison counter n (not shown in the diagram), which is a software counter for counting the number of times that a comparison has been made, is cleared to "0" by the user determination unit 37 (step S1). Then, the user determination unit 37 randomly retrieves one registration keyword from the (keyword registration field 33 of the) keyword/password table 32 shown in Fig. 2 which has been created in the registration file 31 corresponding to the user ID "ocean" (which was inputted by operations from the terminal 2) of the user who performed the login request, and by displaying this on the terminal 2, the user is prompted to input the keyword and its corresponding password (step S2). Here, the keyword "season" has been retrieved as shown in Fig. 3 and this is displayed on the terminal 2.

[0022]

When the keyword is displayed on the terminal 2, the user inputs the password which corresponds to that keyword using the terminal 2. Here, since "season" is being displayed as the keyword, a legitimate user would input "summer", which corresponds to "season", as the password (see Fig. 3).

[0023]

At the user determination unit 37, the password inputted from the terminal 2 corresponding to the keyword display is inputted (step S3), and a comparison is made between this inputted password and the password that is registered in the password registration field 34 in the keyword/password table 32 for the displayed keyword (step S4). If both passwords do not match each other, then the user determination unit 37 assumes that the login request is from an illegitimate user, and thus it does not grant permission to log in.

[0024]

On the other hand, in a case where it is determined that both passwords do match each other as a result of the comparison at step S4, the user determination unit 37 causes the comparison counter n to increase by 1 (step S5). Then the user determination unit 37 determines whether or not this value which is produced after being increased by 1 (here, this is "1") equals a security level that has been set in a security level configuration unit 36 (step S6). Now, assuming that the security level of the computer system 3 is "2", the determination rendered at step S6 will be NO. In this case, the user determination unit 37 returns to step S2 and randomly retrieves one registration keyword (excluding the keyword that was just retrieved previously) from the (keyword registration field 33 of the) keyword/password table 32, and then displays this on the terminal 2. Here, "project" is retrieved as the second keyword,

as shown in Fig. 3, and then this is displayed on terminal 2.

[0025]

When the second keyword is displayed on the terminal 2, the user uses the terminal 2 to input the password which corresponds to that keyword, just as with the first keyword. In the current example "project" is being displayed as the keyword. Thus, the legitimate user would input "language", which is paired with "project", as the password (see Fig. 3).

[0026]

At the user determination unit 37, the password inputted from the terminal 2 is inputted (step S3), and then the user determination unit 37 compares this inputted password with the password that is registered in the keyword/password table 32 for the displayed keyword (step S4). If both passwords do match each other, then the user determination unit 37 causes the comparison counter n to increase by 1 (step S5). Then, the user determination unit 37 determines whether or not the value of n after being increased by 1 (which is "2" here) matches the security level (which is "2" here) indicated in the security level configuration unit 36 (step S6). If these do match each other, as in this example, then the user determination unit 37 assumes that the number of passwords indicated by the security level were inputted sequentially and corresponding correctly to the randomly retrieved registration keywords, and that therefore the login request was from a legitimate user for that security level.

Thus, the user determination unit 37 allows the login to the computer system 3.

[0027]

Note that in the embodiment mentioned above, explanations were given with respect to the case where the number of passwords which need to be inputted is directly indicated by the security level set in the security level configuration unit 36. However, the present invention is not restricted to this embodiment. A configuration may also be used such that the number of passwords which must be entered increases as the security level becomes higher.